

*The following article was originally published in The Business Lawyer, Volume 57, No. 1, November 2001, published by the American Bar Association, Section of Business Law. It has been reproduced here by permission. All rights are reserved. This information or any portion hereof may not be copied or disseminated in any form or by any means or downloaded or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.*

## **From Mount Sinai to Cyberspace: Making Good E-Business Records**

*By Randolph A. Kahn and Diane J. Silverberg\**

### **INTRODUCTION**

From biblical times through the present, society has depended on records to prove the existence of its transactions and agreements. Whether the records were "written in stone," sealed in wax, or notarized, the goal was the same: to create accurate and reliable records.

Creating records with evidentiary force and effect in today's world of electronic records poses special challenges, particularly when, due to the structure of computing technologies, an electronic record's content may comprise a record separate and distinct from its form – to the extent the record's form has even been retained in the first instance. A review of the history and purpose of a record, however, underscores that today's definition of a record, whether evidentially or in the context of the Uniform Electronic Transactions Act (UETA), the Electronic Signatures in Global and National Commerce Act (E-SIGN), or the Government Paperwork Elimination Act (GPEA), relies upon the same notions of reliability, accuracy, and trustworthiness that have existed since the time of Moses.

### **RECORDS' ANCIENT HISTORY**

Whether cave drawings were used to memorialize agreements – and the extent to which those drawings constitute reliable, accurate, and trustworthy accounts of anything other than the artist's imagination – is not susceptible to any sort of definitive answer. Far more certain, however, is that society was concerned with the creation of durable, reliable records throughout most of what is referred to as the written human record.

In the Book of Exodus, Moses meets with God on Mount Sinai and descends the mountain with "two Tablets of the Testimony in his hand, Tablets inscribed on both their sides; they were inscribed on one side and the other. The Tablets were God's handiwork, and the script was the script of God, engraved on the Tablets."<sup>1</sup> Later, as recounted in the Old Testament, when the

---

<sup>1</sup> *Exodus 32:15-16.*

\*Randolph A. Kahn, Esq., Kahn Consulting, Inc. and advisor to PureEdge Solutions, Inc., Legal and Compliance Practices Group; and Diane J. Silverberg, Esq., Kovitz Shifrin & Waitzman.

tablets were destroyed, God commanded Moses to carve two replacement stone tablets which God is then said to have inscribed with the words that were on the shattered set.<sup>2</sup> That Moses's momentous encounter with God would need to be memorialized in writing due to the importance of the subject matter and would require preservation on a durable trustworthy medium for future reference, thus, were important "evidentiary" considerations already prevalent in biblical times.<sup>3</sup>

In a similar vein, it is also reported in the Old Testament that King Ahaseuerus hanged his officer Haman after learning of his treacherous plot to exterminate the Jewish people. To allay Queen Esther's lingering concerns for the safety of her people, the King advised her:

Behold, I have given Haman's estate to Esther, and they have hanged him on the gallows because he sent [his] hand against the Jews. You may write concerning the Jews whatever is favorable in your eyes, in the name of the king, and seal it with the king's signet, for an edict which is written in the king's name and sealed with the king's signet may not be revoked .<sup>4</sup>

Implicit in this biblical narration is that the spoken word was perceived as inadequate for purposes of communicating certain classes of events or directives. Good records, as evidence of important proclamations, activities, or events, were needed to provide confidence that the King's rules would be followed, that significant events would be acknowledged, that transactions would be upheld, and that the laws were authentic. In other words, directives of the ruler rose to the level of requiring a better piece of evidence.

Likewise, during the time of the ancient Roman Empire, scribes, later to become known as notaries, enjoyed elevated status because of their high level of education at a time when few people were literate.<sup>5</sup> They served as public officials charged with responsibility for, among other things, drafting and authenticating documents, as well as overseeing transactions to protect the parties thereto.<sup>6</sup> Notaries are believed to have provided the officially recognized document authentications and archives for the Roman Empire.<sup>7</sup>

The use of a seal, too, has long been a hallmark of authentication, likely predating even writing.<sup>8</sup> Seals, while originally used to secure the contents of jars and boxes, came to serve a

---

<sup>2</sup> *Id.* at 34:1.

<sup>3</sup> This account is believed by some to have taken place approximately 3,300 years ago.

<sup>4</sup> *Esther* 8:7-8.

<sup>5</sup> Jacqueline O'Neal, *The Notary: Yesterday, Today and Tomorrow* (Mar. 2, 1996) (presented at the 1996 LNA Convention), available at [http://www.lna.org/l\\_esprit/oneal.htm](http://www.lna.org/l_esprit/oneal.htm).

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

number of purposes, including as a mark of ownership and to show a grant of authority.<sup>9</sup> Examination of Qumran<sup>10</sup> and the Dead Sea Scrolls confirms this early awareness of the importance of "authentic" records. Samaria papyri found in caves near Jericho, written in Aramaic and dating back to the mid-fourth century B.C.E., were comprised primarily, if not exclusively, of legal documents. Many, it has been noted, still bear official clay seals.<sup>11</sup>

To what effect were these writings, seals, and/or notarizations? In the case of King Ahaseuerus, his written edicts were the law. His utterances – through his written directives – were no different than today's laws. Without the King's signature, the edict penned by his wife, Queen Esther, presumably would have lacked the necessary authority. Even if the King's signature had appeared on a writing, unless accompanied by the seal contained on the King's unique ring, the signature could have been labeled a forgery. Society understood even then that a writing was needed to show the King's directives. It was understood that the directive could be a fabrication without the King's signature. Proof that the signature was authentic, and therefore trustworthy, required more by way of security; thus, the King affixed a seal created by melting a wax-like substance and pressing the seal of his unique signature ring into the wax.

The expansion of the Roman Empire increased the need for records that gave their owner the necessary confidence in their authenticity, trustworthiness, and ability to protect their interests.<sup>12</sup> Where business previously had been transacted as between parties who lived within the same community – where prior dealing and societal pressure to maintain one's reputation would obviate the need for a comprehensive writing in many instances – there became an increasing need to have robust documentation of any business relationship.<sup>13</sup> In other words, the more geographically disconnected people became, the greater the need for a better record of the business transaction.

#### TODAY'S GLOBAL MARKETPLACE

Business and government today function in an anonymous electronic way – where information flows freely around the globe and where business partners can be introduced on a third-party exchange in cyberspace, where no one ever meets, and parties remain faceless throughout their relationship. In such a disconnected world, there is a profound need to have good evidence available to document business events.

Today's ubiquitous e-business really has nothing to do with the dot-com craze. Indeed, there are a whole host of internal business processes (human resource functions, sales information, e-filing with regulators, and the like) that are now done electronically. For each of those transactions, the objective should be to build the same kind of evidence that has been relied

---

<sup>9</sup> *Id.*

<sup>10</sup> *Qumran* is the name by which the ancient ruins on the western shore of the Dead Sea are known today. WEBSTER'S NEW WORLD DICTIONARY 1104 (3d ed. 1988).

<sup>11</sup> *See generally* M.J. WINN LEITH, WADI DALIYEH I: THE WADI DALIYEH SEAL IMPRESSIONS (1997).

<sup>12</sup> O'Neal, *supra* note 5.

<sup>13</sup> *Id.*

upon for thousands of years in the "paper world." If good paper-based evidence was not needed because of legal or business realities, then the analysis should not change merely because the process becomes electronic. Conversely, if a good record was required in the paper environment, then it must be built in the electronic world.

Technological solutions will continue to be offered to help bridge the trust gap that currently exists when doing electronic business in these disconnected times. As comfort grows with doing business solely within an electronic environment, so too will the size and value of transactions increase. As the size and risk of transactions goes up, so too will the need to have trustworthy records memorializing the events and activities increase.

There was a reason for "writing it in stone." Ironically, when that expression was first used, the world was a smaller, more intimate place. Today, where companies are the size of towns and much is at stake, there is a strong need to rely on electronic records that are at least as competent evidentially as conventional paper records. If anything, given the likelihood that a business transaction may end in litigation and a business relationship may sour, there is more need today to have good evidence.

To understand the difficulties in creating and retaining records in a fashion that satisfies evidentiary requirements in today's technological age, one must evaluate the relevant laws (including the seeming laxity in the recent federal enactments and their conflict with recent court rulings), understand the evidence-creation process, and acknowledge the technological limitations that exist as a result of database-centric computing.

## **RELEVANT LAWS**

As noted above, a variety of factors drove society toward development of evidentially sound records. Today's challenge, of determining what constitutes an evidentially sound record in the context of rapidly changing technologies, can be stymied by intimidation by new technologies. When reduced to their essence, however, the rules of evidence and recent laws that speak directly to our evolving technologies are largely consistent with each other, although perhaps not consistent with the courts' interpretation of them.

### **DEFINING "RECORDS"**

Defining what constitutes a record in the first instance is a critical threshold issue, particularly where, in the electronic realm, records can be reduced to data streams, magnetic impulses, and bitmap images. This is particularly important in commerce, where a company will need a record to run its business and prove a transaction, and in the context of litigation, when that company must respond to discovery requests calling for "all records that . . . ." Failing to define a record properly in this context could result in a production response of millions of "records," both paper and electronic (including the jumble of data contained on disaster-recovery tapes) that could effectively bankrupt a company.

UETA and E-SIGN – providing little or no guidance on the definition of a record or electronic record – contain the following definitions. "Electronic record" means a record "created, generated,

sent, communicated, received, or stored by electronic means."<sup>14</sup> "Record" means "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."<sup>15</sup>

The Federal Records Act (FRA)<sup>16</sup> establishes the duties of federal agencies with respect to their creation, management, and disposition of records. For these purposes, the FRA defines "records" as:

all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.<sup>17</sup>

Rule 34 of the Federal Rules of Civil Procedure does not define records, but rather its subset. "Document" includes "writings, drawings, graphs, charts, photographs, phono-records, and *other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form.*"<sup>18</sup>

Whether a record, however defined, constitutes evidence requires a different analysis. A record – whether a writing or magnetic impulse, among other things – that one seeks to introduce into evidence is subject to a number of evidentiary rules. Perhaps most relevant for this exercise is the so-called "best evidence" rule. The Best Evidence Rule was developed to address the admission of fraudulent, fabricated, or incomplete copies of records at a time when the method of making reproductions lacked today's technological consistency and thoroughness.<sup>19</sup>

Specifically, copies originally had to be created by a scrivener, who would have to draft a new original in order to create a copy. Naturally, there was great room for error, inconsistency, and fraud under these circumstances. With the advent of technologies that make it possible to create

---

<sup>14</sup> Electronic Signatures in Global and National Commerce Act (E-SIGN), Pub. L. No. 106-229, § 106(4), 114 Stat. 464 (2000) (to be codified at 15 U.S.C. §§ 7001-7031); Uniform Electronic Transactions Act (UETA) § 2(7) (1999), *available at* <http://www.nccusl.org>.

<sup>15</sup> E-SIGN § 106(9); UETA § 2(13).

<sup>16</sup> 44 U.S.C. §§ 2101-2118, 2901-2910, 3101-3107, 3301-3324 (1994).

<sup>17</sup> *Id.* at § 3301.

<sup>18</sup> FED. R. CIV. P. 34 (emphasis added).

<sup>19</sup> CHARLES T. MCCORMICK, HANDBOOK OF THE LAW OF EVIDENCE 560-62 (Edward W. Cleary ed., 2d ed. 1972).

a precise copy of the original, the insistence on the original is unnecessary in the vast majority of instances. Microfilm, copiers, facsimile machines, and other similar technologies have driven the move to ascribe evidentiary significance to records technically constituting something other than the original.<sup>20</sup>

Ironically, while precise duplicate "originals" can be generated at will, reproducing the complete "four corners" of a complex e-transaction record – like an e-form – is much more challenging.

#### THE FOUR CORNERS OF A DOCUMENT AND THE EVIDENCE-CREATION PROCESS

Historically, a writing has allowed for all information pertaining to the events or agreement memorialized within a record to appear within the four corners of the document. Thus, for example, the content of a business agreement and the fact that it is a contract can be determined from the face of the writing. All the terms would be contained within the writing. Signatures would be affixed to the bottom of the document delineating the end of the agreement, below which nothing could be added. Notaries' markings or seals could be affixed, again, all within the four corners of the writing.

While the notion of having all the parts of an agreement – content, physical form, font size, color, signatures, etc. – contained within one physical and logical document is hardly a revolutionary concept, the notion of "record-togetherness" becomes acutely important and complex in the e-business world. Even if a record appears to be one document, it usually is comprised of a number of separate and distinct electronic files. The four corners of the document or contract allowed the record's content (i.e., what it said) to be displayed to elucidate the document's context (i.e., why the document came into existence and what it was) which could be merged with the record's structure (i.e., physical appearance, font, color, fields) into one physical space, thereby creating a trustworthy and complete record. These notions of content, context, and structure dictate the value of a record, which in turn dictate its evidentiary significance in this technological age.

Having an electronic record is quite different than having a *complete, trustworthy, and authentic* electronic record. The paper world was black or white; either there was a business record documenting some event or transaction, or there was not. The world of e-records, however, is replete with shades of gray. At one end of the spectrum, there are records that are not particularly useful compilations of data. At the other end of the spectrum, there are very good reliable electronic records that possess all the indicia of acceptable evidence. In fact, having a trustworthy electronic record, in many instances, requires much more than the mere content; "[w]e also must have a plan for preserving transmission and receipt data as well as other contextual

---

<sup>20</sup> Nonetheless, if an issue arose as to the actual content of the record, the Best Evidence Rule could be asserted to challenge the admission of the copy without the original. The party offering the record would have to produce the original or come up with an acceptable excuse for failing to present the original. Acceptable reasons for not producing the original have included destruction or loss of the record (without fraud on the part of the offeror), third-party control of the record, the fact that a document is a public record, etc. *Id.* at 569-72.

information. Without this we will not have a complete record.<sup>21</sup> Ensuring that one retains the latter type of record, one with all the necessary evidentiary components, requires effort and forethought, as made clear by many of the new e-record and e-signature laws.<sup>22</sup>

For example, merely retaining the content of a transaction without knowing the context for that content – which can often occur with on-line purchases, where the purchase order exists only on the screen – is largely useless. By way of further example, if the word "Dylan" is retained in conjunction with a business transaction, it could refer to the first or last name of the purchaser, salesperson, a product or model name, or the musician. The word "Lily" printed on a white page could be a person's name, type of flower, color, or fragrance. The number "99" could be a year, product number, or quantity. In other words, without the context of the boxes to which the content relates, there is little benefit to the retained data.

In the electronic world, very often, unless directed otherwise, the only part of the record that is retained is the content. Paper records always had content merged with context; one would know from the face of the document what something was and why it came into existence. The e-records world is precisely the opposite; e-records usually consist of multiple packets of data that are often stored in multiple physical locations. Unless efforts are made to retain the content within the context, the chances are more likely than not that the context will be missing, thereby affecting the likely evidentiary value of the record.

A paper-world purchase order would be one physical record with its contents and significance known from a mere review of the face of the document. The all-important evidentiary issues of date of execution, authorized party, subject, quantity, etc., could all be known from a glance. The electronic equivalent could not be more dissimilar.

In the typical e-transaction, whether a form-based website transaction or an on-line filing application, the questions (the boxes to be filled out) would typically not be physically retained with the answers (the inserted data). Thus, the answers would be a separate compilation of data and would most likely not be stored in the same physical space as the questions. The reason for this lack of "togetherness" is quite simple to understand, but not simple to correct. Specifically, the computing world was structured in a database-centric fashion to allow the parsing or separating out of information for various types of uses. Clearly, building good business evidence was not a primary consideration of the technologists who put together these models. Therefore, the content of a record is almost never connected to the structure or form of the record unless the system is implemented to capture both.

---

<sup>21</sup> G.S. HUNTER, PRESERVING DIGITAL INFORMATION 80 (2000).

<sup>22</sup> See, e.g., Use of Electronic Communication and Recordkeeping Technologies By Employee Pension and Welfare Benefit Plans, 64 Fed. Reg. 4,506, 4,508 (Jan. 28, 1999) (notice of proposed rulemaking and request for information) (to be codified at 29 C.F.R. pt. 2520):

In general, the proposed regulation provides that electronic media may be used for purposes of complying with the records maintenance and/or retention requirements of sections 107 and 209, provided: (1) The recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records kept in electronic form; (2) the electronic records are retained in reasonable order, in a safe and accessible place, and in such manner as they may be readily inspected or examined . . . .

The types of records at issue are not limited to Internet-based commercial transactions. In fact, the need for good e-record building affects all business units within most governmental and commercial institutions. All sorts of internal business processes have and continue to become automated. As part of the process, an electronic record or some compilation of data is the likely by-product. When an employee seeks to have vacation time through an electronic process, or gets approval for a company purchase, a record is at issue. When a publicly-traded company files a quarterly report with the Securities and Exchange Commission (SEC), there is a record that needs to be retained. When a builder completes a building permit electronically, an e-record is created. When a corporation makes estimated tax payments electronically, an e-record of the signature alternatives is retained (user name and password), as is verification of the transfer.<sup>23</sup>

Because technologists were promoting information functionality, as opposed to trustworthy, accurate, and evidentially-significant e-records, business has evolved to the point where virtually any type of transaction can occur on-line, very often without the creation of the requisite "evidence" should the transaction need to be litigated.

In the context of GPEA, the federal agencies are cautioned to consider the issues of "content, context, and structure" when dealing with the preservation of electronic records.<sup>24</sup> With respect to *content*, the National Archives and Records Administration (NARA) has explained that:

The electronic signature or signatures in a record are part of the content. They indicate who signed a record and whether that person approved the content of the record. Multiple signatures can indicate initial approval and subsequent concurrences. Signatures are often accompanied by dates and other identifiers such as organization or title. All of this is part of the content of the record and needs to be preserved. Lack of this information seriously affects a document's reliability and authenticity.<sup>25</sup>

With respect to *context*, NARA has observed that:

Some electronic signature technologies rely on individual identifiers that are not embedded in the content of the record, trust paths, and other means to create and verify the validity of an electronic signature . . . . This information is outside of the content of the record, but is nevertheless important to the context of the record as it provides additional evidence to support the reliability and authenticity of the record. Lack of these contextual records seriously affects one's ability to verify the validity of the signed content.<sup>26</sup>

Finally, as to *structure*, NARA instructs that:

---

<sup>23</sup> DEP'T OF THE TREASURY, FINANCIAL INSTITUTION HANDBOOK FOR EFTPS (Aug. 2000), available at <http://www.fms.treas.gov/eftps>.

<sup>24</sup> POLICY & COMM. STAFF, NAT'L ARCHIVES & RECORDS ADMIN., RECORDS MANAGEMENT GUIDANCE FOR AGENCIES IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES § 4.2, (Oct. 18, 2000), available at <http://www.nara.gov/records/policy/gpea.html> [hereinafter IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES].

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

Preserving the structure of a record means its physical and logical format and the relationships between the data elements comprising the record remain physically and logically intact. An agency may determine that it is necessary to maintain the structure of the electronic signature. In that case it is necessary to retain the hardware and software that created the signature (e.g., chips or encryption algorithms) so that the complete record could be revalidated at a later time as needed.<sup>27</sup>

It bears noting that in the electronic world you may not be able to prove a document's execution merely by a signature. First, according to E-SIGN, an electronic signature is defined as an "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."<sup>28</sup> That definition arguably could be nothing more than a person's name typed at the bottom of the document. Second, the name will likely not be affixed to the records in the traditional (paper) sense of the word, but rather, will be comprised of a separate record.

It should be noted that E-SIGN allows a signature to be "logically associated" with the record, which would seem to be nothing more than a string of metadata connecting the signature to the underlying content of the record. It is critical in the context of evaluating a record's evidentiary value, then, to retain an electronic record's meta-data to link the record with the signature. Indeed, courts have held that, if meta-data has not been retained, the record is incomplete.<sup>29</sup> If the meta-data is retained, then, in the event of litigation, it could be used to show the computer from which the signature was effectuated or the telephone number routing information where the information was generated. Interestingly, according to UETA, "[a] requirement to retain a record . . . does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received."<sup>30</sup> Thus, UETA disregards the evidentiary significance of certain types of meta-data.

It is important to note, too, that there are numerous kinds of "signatures." The technologically neutral brand of laws that have evolved allow any type of e-signature, provided that it evinces the users' intent to be bound by the alternative to the manual "wet signature." While this allows businesses the freedom to use whatever type of technology they deem necessary under the circumstances, it must be understood that not all e-signatures are created equal. For example, "xxx" at the bottom of an e-mail could be sufficient to satisfy the language of E-SIGN.<sup>31</sup> It does not provide much certainty in terms of actually identifying the signer, and, moreover, it is not sufficiently unique, resulting in easy forgery. Authenticity in that case clearly would be an open question. Similarly, a party's typed name at the bottom of the page would seem to satisfy E-SIGN, but the same concerns about authenticity and trustworthiness would persist.

---

<sup>27</sup> *Id.*

<sup>28</sup> E-SIGN § 106(5) (2000).

<sup>29</sup> *Cf. Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1284 (D.C. Cir. 1993) (expanding, generally, the FRA record retention requirements to include the complete electronic record of e-mail communications).

<sup>30</sup> UETA § 12(b) (1999).

<sup>31</sup> *See supra* note 28 and accompanying text.

There are, however, more secure e-signatures that could provide greater confidence that the signer is who he/she claims to be, thereby minimizing concerns about repudiation, contracting with minors, and other such issues. For example, biometric signatures – unique physical attributes, like eye scans, fingerprints, and voice scans<sup>32</sup> – would satisfy E-SIGN and would also provide much greater comfort in the authenticity of the signature alternative and the identity of the signer. Similarly, use of digital signatures (asymmetric cryptography or encryption sometimes referred to as Public Key Infrastructure or PKI),<sup>33</sup> combining private and public keys, allows information to be sent in an encrypted form and secured from alteration during transmission, but also allows parties to sign a contract with the use of the private key. Assuming there are controls in place regarding the issuance of digital certificates (what determines who owns the private key), use of the key pairs and access controls, a recipient of a document signed with a digital signature can have significant comfort that the signature is authentic and that the user cannot easily repudiate the transaction.

Utilizing electronic signatures will require controls and procedures to ensure that e-signatures are used properly and with authorization. For example, if a user name and password are being used in place of a handwritten signature on a paper form to allow employees to change the type of investment or beneficiary on their retirement plan, then there must be tight controls around access to employees' user names and passwords to be able to prove that it was the authorized employee, and not another person with access to the system, that effectuated the change. Additionally, meta-data will be crucial to show from where the change was made, from what computer or telephone number, and other such relevant information. Such ancillary information, if captured, can provide great support and evidence for the event. Failing to have the meta-data makes proof of authenticity harder and may undermine the transaction by forcing a party to rely on a signature whose integrity can be easily challenged.

Decisions regarding the type of electronic signatures to be utilized should be made with ample consideration given to future reliance on the record and the company's ability to prove identity and authenticity, thereby preempting issues that may arise regarding the veracity of the signature or true identity of the signer. In that regard, there is a need to understand the relative merits of the various kinds of e-signatures to be able to make the right choice for the application at issue.

In a typical e-business transaction, the record will likely consist of a separate file for the e-signature technology and multiple other parts regardless of the type of e-signature used. That

---

<sup>32</sup> OFFICE OF MANAGEMENT AND BUDGET, IMPLEMENTATION OF THE GOVERNMENT PAPERWORK ELIMINATION ACT § 7 ( a ) , available at <http://www.whitehouse.gov/omb/fedreg/gpea2.html>.

<sup>33</sup> There is substantial confusion in the terminology surrounding electronic signatures. Laws and commentators often use the words "electronic signatures" and "digital signatures" synonymously, but they are not. *Electronic signatures* refer to a broad category of things that would include digital, digitized, biometric, user name and password, etc. *Digital signatures* fall under a subset that uses asymmetric cryptography, which does not resemble a signature at all. Rather, digital signatures are codes that use a mathematical algorithm to encrypt the message. The use of the private and public key pairs is also used to indicate the identity of the holder of the private key. A digitized signature occurs when you manually write your signature, but the image is captured by a computer and can be subsequently affixed to a document. Control and improper use of digitized signatures are real issues. *Id.* § 7(b)(2).

separate file, and the various separate files comprising the record, will require special management to be considered evidentially sound. Put simply, in the electronic world, the "four corners" concept is gone. The record's "oneness" does not exist. Instead, records are comprised of separate e-files stored in separate computers, perhaps stored in separate physical locations that together make up one record. To have one encapsulated record with the requisite content, context, structure, meta-data, and e-signature, requires the forethought to build a record, rather than simply allowing it to happen, and is a function of technological ingenuity and business decisions.

#### TECHNOLOGICAL LIMITATIONS

Further confounding the process, the applications, formats, or computer languages that have become popular in the electronic age do not possess the ability to retain and structure data in the "four corners" kind of way that has traditionally been the hallmark of trustworthy complete records. For example, HyperText Markup Language (HTML) retains content, but has difficulties with retention of the template that determines how people may have seen the record online.<sup>34</sup>

What people see, of course, can be a critical issue. For example, according to the new privacy regulation for the securities industry, notice of a brokerage company's privacy policy must be clear and conspicuous.<sup>35</sup> Similarly, states often have requirements of conspicuousness for such contractual provisions as disclaimers, arbitration clauses, jurisdiction-selection clauses, and waivers of jury. If the party seeking to enforce the contractual provision cannot demonstrate such conspicuousness to the trier of fact because the e-record's content cannot be aligned with its original context and the original physical presentation (because it no longer exists), the proponent of the provision will likely fail. In other words, changing the context of the content can have a dramatic effect upon ultimate meaning and understanding and, thus, upon success in proving the transaction.

E-SIGN indicates that whenever any law requires that a record be retained, it can be retained in electronic form, provided that it: (i) accurately reflects the information in the record; (ii) remains accessible to all whom by law are entitled to access the record; and (iii) remains capable of accurate reproduction.<sup>36</sup> E-SIGN makes clear that a record that meets these criteria is considered an "original."<sup>37</sup> The requirement to retain an e-record that accurately reflects the information in the record could be construed to require that only the content of the record be retained. The language of E-SIGN could have mandated the retention of a "complete trustworthy record" which, presumably, would have required the retention of the whole record, not just the "information in the record."<sup>38</sup> This interpretation is important because it appears to allow decisions

---

<sup>34</sup> See, e.g., COHASSET ASSOCS., INC., ELECTRONIC COMMERCE TRANSACTIONS: REQUIREMENTS, ISSUES, AND SOLUTIONS (2000), at [http://www.cohasset.com/main/library/coh\\_articles/index.htm](http://www.cohasset.com/main/library/coh_articles/index.htm).

<sup>35</sup> Regulation S-P: Privacy of Consumer Financial Information, 17 C.F.R. § 248 (2001).

<sup>36</sup> E-SIGN § 101(d) (2000).

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

to be made about what to retain, thereby possibly allowing technological expediency at the expense of good evidence.

Of particular interest on this issue is the decision in *Public Citizen v. Carlin*<sup>39</sup> and the court's observation that:

[E]lectronic records often contain information that is not preserved in a printout, record or even in other computerized systems of records. For example, paper print-outs of computer spreadsheets only display the results of calculations made on the spreadsheet, while the actual electronic version of the spreadsheet will show the formula used to make the calculations . . . . Some word processing systems allow users to annotate a document with "a summary" or "comments" that contain information on the author of the document, its purpose, the date that it was drafted or revised, and annotations by authors or reviewers. These comments, however, usually do not appear on a printed copy of the record. Such differences between electronic and paper records illustrate the fact that the administrative, legal, research and historical value of electronic records is not always fully captured – indeed, is usually not captured-by paper or microfiche copies. Electronic records therefore do not become valueless duplicates or lose their character as "program records" once they have been printed on paper; rather, they retain features unique to their medium.<sup>40</sup>

While this decision was overturned on appeal on different grounds, the lower court makes clear that, in its opinion, the electronic record is comprised not only of its content and its physical presentation, but of the unique functionality of the software behind the record, as well. Such an interpretation of E-SIGN further supports the notion that, given the complexities of computing environments, retaining a "complete electronic record" in much the same way as a paper document with all that is part of the "four comers," is not simple in the electronic context.

Stated differently, keeping the content is easy in a database-centric computing environment, but keeping the content with the form of the document, attached to the electronic signature, together with the logic of the document, is not easily accomplished and may be cost-prohibitive, given the subject of the transaction.

In line with other recent legislation that promotes the use of information technology, but does not require the use of particular technologies, E-SIGN continues the trend of technological neutrality. There are three likely reasons for this trend. First, market forces, not laws or regulations, effectively dictate the use of appropriate technology. Second, a technologically neutral approach will help to ensure that legislation remains relevant as technology changes over time. Third, technological neutrality assumes that the level of security provided by the e-record used to document the transaction should be directly related to the amount of risk or money involved in the transaction. In fact, NARA characterizes trustworthy records as follows:

Reliability, authenticity, integrity, and usability are the characteristics used to describe trustworthy records from a records management perspective. An agency needs to consider

---

<sup>39</sup> 2 F. Supp. 2d 1 (D.D.C. 1997).

<sup>40</sup> *Id.* at 14 (citing Comments of Public Citizen on NARA Proposal to Revise General Records Schedule 20, 1 ADMIN. REC. 205, available at <http://www.citizen.org/litigation/briefs/ERecords/articles.cfm?ID = 614>).

these characteristics when planning to implement an electronic signature technology so that it can meet its internal business and legal needs, and external regulations or requirements. The degree of effort an agency expends on ensuring that these characteristics are attained is dependent on the agency's business needs or perception of risk.<sup>41</sup>

Implicit in E-SIGN's advancement of the notion of technological neutrality is that creators and users of records are in the best position to assess their own business needs, and can build and retain a record that accommodates their requirements. This is not to say, however, that a decision to retain only raw data even if it may satisfy the new e-record laws and regulations from an admissibility standpoint will necessarily satisfy the rules of evidence in terms of credibility, competence, and sufficiency. In that regard, while UETA may not require the retention of transmission-related meta-data,<sup>42</sup> it would appear that other laws, such as the Food and Drug Administration (FDA) regulation<sup>43</sup> dealing with electronic records, would require at least certain types of meta-data to address issues of authenticity, trustworthiness, and related concepts. Certainly in the context of the federal government, courts have concluded that meta-data constitutes an important part of a record and that it must be retained.

Specifically, in *Armstrong v. Executive Office of the President*,<sup>44</sup> the U.S. Court of Appeals for the District of Columbia observed that meta-data is an essential part of an e-mail record.<sup>45</sup> The court commented that "[w]ithout the missing information [meta-data], the paper print-outs – akin to traditional memoranda with the "to" and "from" cut off and even the "received" stamp pruned away – are dismembered documents indeed."<sup>46</sup>

What *Armstrong* points out, among many other things, is that building and/or retaining a sufficient and complete e-record requires an acknowledgment of the technical limitations of the computing devices and the foresight to structure such systems to capture and retain the complete record. While the record in the paper world merely existed, in the cyberworld, good records have to be built, and the reality is that neither government nor business has been in the business of building good electronic evidence from the outset.

While E-SIGN and UETA promote the use of electronic records without any meaningful guidance on what constitutes good evidence, there are industry regulations and other such related guides that are far more instructive. For example, the FDA electronic record/electronic signature rule advises that when using an e-signature, the meta-data must be captured "linking" the signature

---

<sup>41</sup> IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES, *supra* note 24, § 4.1.

<sup>42</sup> UETA § 12(b) (1999) ("A requirement to retain a record . . . does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.").

<sup>43</sup> FDA, Electronic Records; Electronic Signatures, 21 C.F.R. § 11 (2001).

<sup>44</sup> 1 F.3d 1274 (D.C. Cir. 1993).

<sup>45</sup> *Id.* at 1284.

<sup>46</sup> *Id.* at 1285.

to the record.<sup>47</sup> Specifically, "electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means."<sup>48</sup> It also should be noted that under the general requirements for electronic signatures each electronic signature must be "unique to one individual and shall not be reused by, or assigned to, anyone else," and "[b]efore an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature . . . the organization shall verify the identity of the individual."<sup>49</sup> These requirements are clearly more restrictive than that of either E-SIGN or UETA and suggest that the FDA-regulated world is creating a higher threshold for what is an acceptable signature and how records and signatures need to be managed technologically and administratively. Similarly, the U.S. Department of Justice (DOJ), has noted that:

the OMB recognizes the strength of Public/Private Key Cryptography in comparison to other electronic signature techniques, and identifies PKI as the strongest method of assuring identity . . . . The OMB guidelines point out that an agency's policies and procedures for the operation and maintenance of a PKI are an essential component of trust that binds a person's identity to a digital signature.<sup>50</sup>

While digital and biometric signatures may provide a greater degree of security and comfort with respect to the authenticity of the signer, there are substantial costs and complexities in implementation of both.

The infrastructure policies and procedures around the retention and security of e-records are essential to their long-term trustworthiness, accessibility, and completeness. As reflected above in the DOJ's comments, as well as in the FDA regulations, controls to ensure "the integrity of system operations and information stored in the system"<sup>51</sup> will be essential to usable e-business records. In that regard, the regulations mandate various procedural protections to ensure record integrity. Such safeguards include: system validation; archival protections; computer-generated, time-stamped audit trails; use of appropriate controls over system documentation; and comprehensive training.<sup>52</sup>

---

<sup>47</sup> 21 C.F.R. § 11.70 (2001).

<sup>48</sup> *Id.*

<sup>49</sup> *Id.* § 11.100.

<sup>50</sup> DRUG ENFORCEMENT ADMIN., U.S. DEP'T OF JUSTICE, COMPLIANCE WITH FEDERAL STANDARDS AND REQUIREMENTS § 8.1.3 (Oct. 13, 2000), *available at* [http://www.deadiversion.usdoj.gov/ecomm/csos/concept/section8/8\\_1\\_3.htm](http://www.deadiversion.usdoj.gov/ecomm/csos/concept/section8/8_1_3.htm).

<sup>51</sup> Electronic Records; Electronic Signatures, 62 Fed. Reg. 13,430, 13,430 (Mar. 20, 1997).

<sup>52</sup> 21 C.F.R. § 11.10 (2001).

## **CONCLUSION**

In the face of this most disconnected environment, where trust is rarely a given, technology, law, and evidence have some of their greatest challenges. In that regard, it is a confluence of events which provides great opportunity and potentially disastrous challenges. In this time of faceless transactions, businesses need some of the best evidence on which to rely if and when relationships sour.

Even if the new generation of e-records and e-signatures laws have given businesses the luxury of making their own determinations as to the precise form of record to be retained, incomplete, untrustworthy records will be excluded from evidence or otherwise attacked as lacking integrity. Therefore, merely because compliance with E-SIGN and UETA is easy does not mean that creating good e-evidence will be easy.

On the one hand, companies should be loathe to spend enormous resources to save vast quantities of e-data that, in the end, may be usable for certain purposes, but fail to constitute "good evidence," and ultimately fail to protect the business and legal interests of the institution. On the other hand, as applications are built, business decisions need to be made about what kind of evidence to build based upon a quantification and qualification of cost and risk.